HIGHLY ACCURATE SECURITY AND FILTERING SOFTWARE

Priority information:

This patent application is a continuation-in-part patent application of (a) the presently pending United States Patent application no. 09/661,876 ("Web-Based Security and Filtering System with Proxy Chaining") previously filed by Applicant and Inventor Joshua Haghpassand on September 14, 2000 and which is incorporated herein by reference in its entirety

Field of the Invention

The field of this invention is software, and more particularly, highly accurate security and filtering software.

Background of the Invention and Discussion of the Prior Art

Currently, access to the Internet and the use of e-mail has created various gaps in security which threaten families, consumers and corporations. Parents and corporations need to properly control the users' access to the disapproved contents and to web sites that are deemed untrustworthy. While there are tools in the market, none have fully resolved the problem. Such tools may excessively filter content and web sites to an extent that they even do not allow the user access to some valuable and useful web sites. This is called the filtering accuracy, and currently, none of the available products can reach to 100% accuracy.

In addition there are other risk factors to the user and corporate data, which may violate the user privacy preferences. For example, the existence of snoopers, eavesdroppers, remote and local intruders, Spyware (software programs and agents are installed on the user computers without their knowledge and act as Trojan horse on the user computers to steal user information, monitor the user behavior and transmit the information to their senders), impersonators (use the

computer address for their own use for sending Spam emails or other activities), hijackers (take control of the computer resources for unauthorized use such as providing pornography services for their own clients), computer viruses, and etc., create real threats to the user information and privacy. Some web sites collect the user information and transmit the information unprotected over the wire. This allows the snoopers and eavesdroppers to use such information.

E-mail systems are abused data mining engines and eavesdroppers.

Further, there are factors that create disturbance, and waste valuable resources. This includes email Spams, disrupting advertisement pop-up windows.

Some additional privacy violations are imposed by obtaining the user information from unauthorized users and children. Some web sites even collect very secure information from children.

Additional drawbacks associated with the current systems include the fact that they require significant maintenance and configuration requirements. Since there are no single products that answer all the problems together, the user may need to install several products to reach a fairly successful performance.

SUMMARY OF THE PRESENT INVENTION

The software of the present invention solves these threats and shortcomings. It provides one integrated solution with the additional quality of service and privacy protection. It stops unauthorized users and children to disclose the secured information on the web. It provides a 100% accuracy in a fully web access filtering system that allows parents and corporate to rate the web sites along the trusted and distrusted line, with the additional filtering over the contents that are provided via trusted web sites.

The software of the present invention protects computer user from web sites that violate user privacy, and place Spyware agents on user computers. It protects the computer system against local and remote intruders, where the file system will be securely locked and the contents are securely encrypted. Additionally, it protects the computer resources from unauthorized remote access by only allowing the access to the trusted clients and visitors from the trusted domains and addresses.

The software of the present invention allows email users to stop Spam emails, and protect children and corporate email users from receiving e-mails from distrusted email senders, ISP domains, and with the inappropriate subjects. The software prevents disapproved remote access to the computer for identity impersonations. It allows the remote users to become anonymous on the cyberspace. It allows the local user to become anonymous on the cyberspace with the use of proxy chaining.

The email senders may protect fully or portions of their email messages, and attachments and store or exchange the encryption keys with the email recipients with no electronic storage or transmission requirements. On the other hand, they have the option of also using very complex encryption keys to encrypt their computer file systems. The software of the present invention prevents the computer file system corruption from multiple encryptions by allowing encryption ownership for each file. The person who encrypts a file (without keeping the original copy) in the computer, will also own the file until decrypting the file. No other user on the same computer may be allowed to encrypt the already encrypted file.

This software product allows web users to shut down the embedded 'script language' contents within the page resources. This prevents the use of powerful scripting languages within

the web pages from processing user information and transmit them without corporate or parents permission and knowledge.

This software can be used automated, and it can be used as a background service in the operating system. This allows the application server to be launched as an automated service after the computer is turned on (booted up). The automated list update provides a maintenance free system.

This software product supports the user of proxy chaining. This enables the network architects to use the product in various network setups to fully take advantage of its functionalities, and its privacy protection and its security tools.

This software product conforms to all types of Internet connection requirements (DSL, Modem, Cable, LAN), and all the ISP's requirements (Use of 'automated configuration script', or use of external proxy servers), and to all the available browsers in the market.

In sum, the software of the present invention is a security software comprises administrative module for configuring access levels and creating types of accounts and application server for domain filtering by checking against friendly and unfriendly inbound, outbound and exception lists. Hard filtering either approves, terminates requests or re-routes request without the user's knowledge. Soft filtering passes approved and disapproved requests, but when passing disapproved requests and queries, an e-mail alert is sent to authorized recipients.

Content filtering includes checking a content of a requested document against a friendly, unfriendly list and exception list. Hard filtering against a friendly list passes or rejects the requested document. Soft filtering against a friendly list passes the requested document if it rejects the content. If the soft filtering approves the content then it highlights the content. Options

include e-mail filtering that checks subject, sender's address and domain against an unfriendly, friendly and exception list. e-mail alert for hard filtering, inbound privacy shield, a pop up blocker, the application server acts as proxy server with proxy chaining capabilities. An encryption function can encrypt part of or a full e-mail message, attachment, file or file system.

The software of the present invention is a fully automated and programmable maintenance free filtering and monitoring system capable of using up to 48 different sets of complete and customized operational configurations during a daily operation. As part of automated services used by the domain and content filtering engines and by the automated list update module, an optional e-mail alert allows the software of the present invention to periodically send e-mail messages to the parents or administrator regarding user violations after the queue of the e-mail alert system has accumulated a certain number of such messages that need to be sent. After sending the contents of its queue it cleans the queue. The e-mail alert system also sends an e-mail to the parents or administrator whenever the lists have been updated.

IMPORTANT OBJECTS AND ADVANTAGES

The following important objects and advantages of the present invention are:

(1) to provide a software that filters using exception lists and thereby achieves accuracy up to 100% by preventing over-filtering;

(2) to provide a security and filtering software that includes an encryption function that allows the user at his option to encrypt only a portion of an e-mail message, file or attachment;

(3) to provide a software that includes an encryption function that evades eavesdroppers that employ data mining programs or processes;

(4) to provide a software that includes an encryption function that employs an encryption

key that at the option of the user can be either binary and therefore hard to decipher or character text that is hard to obtain since it can be communicated discretely orally;

(5) to provide a security and filtering software that can be used by a remote or local user;

(6) to provide a security and filtering software that can simultaneously halt eavesdroppers, highjackers, intruders and impersonators;

(7) to provide a security and filtering software that performs hard and soft filtering;

(8) to provide a security and filtering software that has the option of blocking unwanted pop-ups;

(9) to provide a security and filtering software that can be used to block spam e-mails;

(10) to provide a security and filtering software that includes e-mail filtering;

(11) to provide a security and filtering software that includes a privacy shield to protect sensitive information;

(12) to provide a filtering and security software that has a domain filtering engine that can provide an optional e-mail alert system for both hard and soft filtering;

(13) to provide a security and filtering software that can block spyware;

(14) to provide a security and filtering software that can perform both content and domain filtering;

(15) to provide a security and filtering software wherein its content filtering can replace a requested document that has been rejected with a replacement document selected by a user;

(16) to provide a security and filtering software that allows a user to enhance searching capabilities by placing the searched item into his friendly content list and highlight the "hits";

(17) to provide a security and filtering software that can support unlimited numbers of

password protected user accounts with the complete support of personalization;.

(18) to provide a security and filtering software including an automated scheduler that supports 48 different account types during a single day,

(19) to provide a security and filtering software that includes an automated application launcher that is also programmable by the parents or administrator,

(20) to provide a security and filtering software that includes an automated list updater,

(21) to provide a security and filtering software that has a range of access levels from maximum 100% access to full suspension,

(22) to provide a security and filtering software that supports anonymous users in manual mode,

(23) to provide a security and filtering software that includes an application server that can act externally as a proxy server or as a chain of proxy servers,

(24) to provide a security and filtering software whose administrative module can configure an automated configuration script file for accessing the Internet,

(25) to provide a security and filtering software that includes e-mail filtering in which disapproved incoming e-mail can be deleted from a user e-mail inbox or optionally remain in the inbox but be inaccessible,

(26) to provide a security and filtering software in which the automated scheduler can shut down access to the world wide web during certain hours,

(27) to provide a security and filtering software that is ideal for helping parents control their children's access to the world wide web,

(28) to provide a security and filtering software that automatically updates the friendly and

unfriendly user domain lists and is therefore maintenance free,

(29) to provide a security and filtering software wherein the user for filtering purposes can use his own private list, a network list or hybrid of the two,

(30) to provide a security and filtering software that can be used on all types of Internet connections such as DSL, modem, cable and LAN connections,

(31) to provide a security and filtering software that works with all types of web browsers that are available on the market, and

(32) to provide a security and filtering software that corporations and parents can use to get notifications (e-mail alerts) advising them about a pattern of behavior without actually directly affecting the pattern of behavior, such as when their employees or grown-up children visit disapproved web sites or view disapproved contents.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 shows the overall software of the present invention in the context of a network;

FIG. 2 shows the flow of user requests (in the direction of numbers "1" through "9") through the filtering engines and security management features of the software of the present invention;

FIG. 3 shows the application server controlled by the automated scheduler which loads in different user accounts at different times;

FIG. 4A shows either soft filtering or hard filtering by the domain filtering engine of the software of the present invention approving a request;

FIG. 4B shows soft filtering by the domain filtering engine disapproving a request including a mandatory e-mail alert;

FIG. 4C shows hard filtering by the domain filtering engine disapproving a request; including optional e-mail alert;

FIG. 4D shows hard filtering by the domain filtering engine disapproving a request;

FIG. 5A shows hard filtering by the content filtering engine approving a request;

FIG. 5B shows hard filtering by the content filtering engine disapproving a request;

FIG. 5C shows hard filtering by the content filtering engine disapproving a request with an optional replacement document;

FIG. 6A shows soft filtering by the content filtering engine against unfriendly list approving a request;

FIG. 6B shows soft filtering by the content filtering engine against unfriendly list disapproving a request and passing a remainder to the user;

FIG. 6C shows soft filtering by the content filtering engine against friendly list approving a request and highlights components found in the friendly list;

FIG. 6D shows soft filtering by the content filtering engine against friendly list disapproving a request and passes the entire document;

FIG. 7A shows a local user with the software of the present invention;

FIG. 7B shows the software of the present invention used remotely by multiple users

FIG. 8A is a flow diagram showing the application server acting externally as a single proxy server; and

FIG. 8B is a flow diagram showing the application server acting externally in a proxy chaining deployment with multiple instances of the software sequentially connected.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The present invention is a versatile customizable security and filtering software 10 that can be installed on a computer and be used by a remote user who obtains anonymity on a global telecommunications network or by a local user. Alternative embodiments of the software can be used by local users only. The software 10 includes an administrative module 20 and an application server 30. The application server 30 includes both a domain filtering engine 40 and a content filtering engine 50. In certain embodiments, the application server does not include a domain filtering engine.

Software 10 includes an administrative module 20 that a user interacts with for creating user accounts and configuring those user accounts, and for configuring automated services. The administrative module 20 accepts user inputs for configuration settings for inbound communications and for outbound communications, and has list maintenance functions that include list editing, list deleting, searching of lists, saving of lists, proxy chaining routing, adding and deleting users, interchanging lists and importing and exporting lists.

It is noted that any list mentioned herein can be empty.

The administrative module 20 interfaces with the application server via the configuration files and to the e-mail encryption system, as more fully described below. Administrative module 20 is used to configure a range of user access levels and can create three types of user accounts that have unique user names and passwords for each user account including (1) an administrator account that is self-configuring and that controls automated services and selects for each account hard filtering or soft filtering, (2) regular accounts with administrative privileges other than the privilege to create additional accounts, view information on any other accounts or configure automated services and (3) regular accounts without administrative privileges. In addition module

HIGHPASSAND – Highly Accurate Security & Filtering Software

20 can create a fourth type of user account namely one anonymous guest user account to be used in a manual launch of the software by general users who have no system-based user name or password.

The administrative module stores as encrypted files on hardware memory the configurations of the range of access levels for the user accounts created and the configurations of the automated services. The range of access levels ranges from maximum 100% access to full suspension. As explained below, the automated scheduler can shut down access to the world wide web by shutting down the proxy server. On the other hand, it can use various user accounts with a whole range of limitations. For example, if a user's unfriendly list is empty, there is no limitation on access to any domain on the world wide web.

The administrative module 20 is also capable of configuring an automated configuration script file for accessing the global telecommunications network. This use of automated configuration script conforms to similar configurations on the user browser.

Application server 30 includes a domain filtering engine 40 that is capable of using from the encrypted files a friendly outbound list and an unfriendly outbound list only one of which is active at any given time and an outbound exception list, and is capable of using a friendly inbound list and an unfriendly inbound list only one of which is active at any given time, and a domain inbound exception list. The friendly outbound list, the unfriendly outbound list, the friendly inbound list, the unfriendly inbound list, the outbound exception list, the domain inbound exception list, the friendly e-mail list and the unfriendly e-mail list are uniquely configured for each user account.

The domain filtering engine 40 is capable of registering the request in a logfile of all web

sites requested by a user and capable of performing domain filtering.

Domain filtering engine 40 for inbound requests checks the identity of a requesting remote client against the friendly inbound or unfriendly inbound list and domain inbound exception list maintained in the encrypted files. Similarly, for outbound requests domain filtering engine 40 checks local user and remote user requested domains, URLs and links against the friendly outbound list, unfriendly outbound list and outbound exception list. Then with respect to both inbound and outbound requests if the user has elected to have the domain filtering engine perform 40 hard filtering unless it is overruled by the outbound exception list or domain inbound exception list (which can only happen if it is rejected by an unfriendly list or approved by a friendly list) it either approves the request, terminates the request or re-routes the terminated request without the knowledge of the user. If the user has elected to have the domain filtering engine 40 perform soft filtering then unless overruled by the outbound exception list or domain inbound exception list (which can only happen if it is rejected by an unfriendly list or approved by a friendly list) it passes disapproved requests and periodically sends an e-mail alert to authorized recipients regarding the disapproved request after a certain amount of time.

The domain filtering engine also has an optional e-mail alert component or system for hard filtering and for soft filtering. Periodically, the e-mail alert component sends the e-mail alerts that have accumulated in its queue during the time period to parents or other administrative users regarding the users' access violations, time of the violation, web address attempted to be accessed and the user name. The e-mail alert contains the user-violated domain names, the date of violation and the user name. The e-mail alert system then cleans its queue.

With respect to domain filtering, inbound communications are arranged so that an actual

location of a highly sensitive resource is located in an unpublished location that is a replacement location to which requests rejected by the application server are rerouted, wherein approved users are listed in the application server in the unfriendly inbound list and are sent by the application server to the replacement location, and wherein unapproved users are not listed in the unfriendly inbound list and have their request sent to a published address that contains harmless information.

Content filtering engine 50 is capable of performing content filtering which includes checking a content of a requested document against a friendly content inbound list, an unfriendly content inbound list, and a content exception list taken from the encrypted files. The friendly content inbound list, the unfriendly content inbound list and the content exception list being uniquely configured by each user. Only one of the friendly content inbound list and the unfriendly content inbound list is active at any given time.

It should be noted that for each engine, namely the domain filtering engine 40 and the content filtering engine 50 the user can select whether he wishes hard filtering or soft filtering. The term "requested document" as used herein refers to a web page (for example in HTML or XML format) on the world wide web that a user seeks to access or documents downloaded from a web link.

For hard filtering against the unfriendly content inbound list the content filtering engine 50 either passes the requested document if the content of the requested document is not on the unfriendly content inbound list or, unless overruled by the content exception list, rejects the requested document if the content of the requested document is on the unfriendly content inbound list. For hard filtering against the friendly content inbound list the content filtering engine 50 either, unless overruled by the content exception list, passes the requested document if the content

of the requested document is on the friendly content inbound list or rejects the requested document if the content of the requested document is not on the friendly content inbound list. The content filtering engine, when performing hard filtering, can also replace a requested document that has been rejected with a replacement document selected by a user of the administrator account

If the user has selected soft filtering for the content filtering engine, then if the content filtering engine 50 is checking the content of the requested document against the unfriendly content inbound list it either approves the content of the requested document and passes the full requested document if the content is not on the unfriendly content inbound list or, if the content is on the unfriendly content inbound list then, unless overruled by the content exception list, rejects the content of the requested document and passes a remainder of the requested document. For soft filtering against the friendly content inbound list the content filtering engine 50 either, unless overruled by the content exception list, passes the full requested document if the content is not on the friendly content inbound list or passes the full requested document and highlights the content of the requested document if the content is on the friendly content inbound list

Content filtering engine 50 also includes an e-mail filtering component that checks a subject, a sender's address and a sender's domain against an unfriendly e-mail list, a friendly e-mail list and an e-mail exception list. For e-mail filtering software 10 includes an option of hard e-mail filtering in which an incoming disapproved e-mail is deleted from a user e-mail inbox and includes an option for soft filtering in which an incoming disapproved e-mail remains in the user e-mail inbox but is inaccessible to the user.

Application server 30 acts internally to communicate with the domain filtering engine 40

and with the content filtering engine 50. Application server 30 also acts externally as a proxy server that receives requests from HTTP clients, forwards the requests to servers, receives a server response and forwards the server response to the HTTP clients. Alternatively, application server 30, instead of acting externally as a proxy server, acts externally in the context of a deployment of a chain of proxy servers (multiple instances of the software are sequentially interconnected). The chain of proxy servers include at least a first proxy server that receives requests from HTTP clients and forwards the requests through a zero or more intermediary proxy servers to a last proxy server, the last proxy server forwarding the requests to servers, and wherein the last proxy server receives a server response and forwards the server response through the zero or more intermediary proxy servers back to the first proxy server, which first proxy server forwards the server response to HTTP clients. As shown in FIG. 8B the series of dots under the phrase "Client request" in the middle of the FIG. 8B means that between zero and "N" intermediate proxy servers may exist between the first and the last proxy servers. One of the proxy servers in the proxy chaining deployment should be an application server running as a proxy server.

Domain filtering engine 40 and content filtering engine 50 each also have a privacy shield. Domain filtering engine 40 has an outbound privacy shield for blocking disapproved character strings representing confidential information. The administrative user, parent or corporation determines the information that is critical to the business or family and should not be disclosed on-line. An example is a social security, date of birth, address, family names, etc. The content filtering engine's 50 inbound privacy shield component blocks scripting language functions for particular user accounts.

Content filtering engine 50 also includes a pop up blocker as an option. The incoming web page's source language is cleaned with respect to any syntax language that would otherwise activate a pop-up window. The user activates this feature by just clicking on a check box.

Software includes an automated scheduler that starts the application server, stops the application server, reloads new user accounts and re-starts the application server continuously. It can also stop the application server to shut down the user's access to the world wide web. The automated scheduler thus controls a launching of the application server automatically and decides which user account to activate.

Software 10 also includes an automated list update module that updates the friendly inbound list, the unfriendly inbound list, the friendly outbound list and the unfriendly outbound lists for each user account from links on the web. The e-mail alert system also sends e-mail alerts to parents and administrators upon the occasions of a successful update by the automated list update module or its failure to successfully update as scheduled (besides the alerts on the occasion of user domain filtering violations, as discussed previously).

In general, the software 10 always automatically uses domain filtering. It cannot be turned off although it can be de-activated simply by using unfriendly inbound and unfriendly outbound lists and keeping them empty. Content filtering, as with all other components except domain filtering, on the other hand can be turned off.

Software 10 has a special encryption utility that can evade data mining programs. The administrative module 20 includes an editor. The editor includes an editing pane. The editor also includes an encryption function that generates one or more secret symmetric encryption keys in two different formats - character text and binary, each having particular advantages. For example,

the binary is harder to decipher and the character text is harder to transmit. The one or more encryption keys are uniquely associated with a text inputted by a user in the editing pane. The encryption component or function is capable of encrypting at the user's option all or only a portion of an e-mail message and all or only a portion of an e-mail message attachment file. The encryption function is also capable of encrypting all or a combination of files on a hard drive local to the software. The binary key is very good for encrypting files on a hard drive, which protects against intrusion attack.

By encrypting only a minimal portion of an e-mail message or its attachment file or a combination of files, the data mining engines are evaded since such engines have recognition tools that recognize the main or most prevalent text that appears in a file or message. Accordingly, when the data mining engine sees that most of the text of the e-mail message, the e-mail attachment file or the combination of files are not encrypted, the data mining engine does not signal that the message or file(s) is something it does not understand since it may be encrypted. On the other hand, since it in fact does not understand the small portion that was encrypted, it ignores that small portion.

Although the invention has been described in detail in the foregoing specification and accompanying drawings with respect to various embodiments thereof, these are intended to be illustrative only and not limiting. One skilled in the art will recognize that various modifications and variations may be made therein which are within the spirit and principles of the invention and the scope of the appended claims. It is not desired to limit the invention to the exact description and operation shown and described. The spirit and scope of this invention are limited only by the spirit and scope of the following claims.